Amendments to the Specification:

Please amend the paragraph beginning on page 8, line 21 with the following amended paragraph:

FIG. 2 shows a block diagram of a portion of a system in accordance with one embodiment of the present invention. It will be recognized that although shown as interfacing with a POD based system, the disclosed method and apparatus can be used with any encrypted data in any suitable system or arrangement. An encryption/decryption module 202 is located between the memory controller 32 and in this example, the local (e.g., off chip or on-chip) frame buffer memory 38. A frame buffer stores information, including but not limited to compressed video, uncompressed video frames, graphics elements from a rendering engine, and frames for display. The encryption/decryption module [[102]] 202 selectively encrypts at least some of the data passing through the encryption/decryption module [[102]] 202 en route to the local frame buffer memory 38 to provide encrypted data, and then stores the encrypted data in the local frame buffer memory 38. Little or no unencrypted data corresponding to the data to be protected is stored in the frame buffer 38. The encryption module 102 also decrypts the encrypted data from the frame buffer 38 and provides decrypted data from the frame buffer 38 to the memory control 32.

Please amend the paragraph beginning on page 9, line 29 with the following amended paragraph:

Accordingly, even if an illicit copier managed to copy or move the data residing within the encrypted memory space to another (external) device such as a writable CD-ROM, ~~Zip drive~~ ZIP® brand storage device, hard drive, or other storage device, the data would be of little or no use to the illicit copier. Only by decrypting the data using the appropriate keys could the illicit copier gain access to the content.